This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing Of Claims

1. (Cancelled)

2. (Cancelled)

3. (Cancelled)

4. (Cancelled)

5. (Original) The method as recited in claim 4, further comprising:

decrypting selected ones of the stored encrypted keys, as needed.

6. (Cancelled)

7. (Currently Amended) The method as recited in **claim 23** ~~**claim 6**~~, further comprising:

receiving a cryptography related command.

8. (Original) The method as recited in claim 7 wherein the cryptography command includes an authentication request and a number of associated authentication request parameters.

9. (Original) The method as recited in claim 8, wherein the authentication request is an HDCP authentication request.

10. (Original) The method as recited in claim 8, further comprising:

retrieving an encrypted authentication key from the non volatile memory

corresponding to the authentication request; and

decrypting the authentication request based upon a corresponding decryption protocol.

11. (Original) The method as recited in claim 10, further comprising:

responding to the authentication request based on the decrypted authentication request.

12. (Cancelled)

13. (Currently Amended) Computer program product as recited in **claim 25** ~~claim 12~~, wherein the key is

one of a plurality of keys and further comprising:

computer code for providing a number of the plurality of keys.

14. (Original) Computer program product as recited in claim 13, further comprising:

computer code for selecting one of the number of available encryption protocols for each of the provided keys; and

computer code for encrypting each of the provided keys based upon a particular one of the selected encryption protocols.

15. (Original) Computer program product as recited in claim 14, further comprising:

computer code for storing the encrypted keys in the non-volatile memory.

16. (Original) Computer program product as recited in claim 15, further comprising:

computer code for decrypting selected ones of the stored encrypted keys, as needed.

17. (Original) Computer program product as recited in claim 13, wherein the plurality of keys includes a decryption key and an authentication key.

18. (Original) Computer program product as recited in claim 17, further comprising:

computer code for receiving a cryptography related command.

19. (Currently Amended) Computer program product as recited in claim 18 wherein the cryptography command includes an authentication request and a number of associated authentication request parameters.

20. (Original) Computer program product as recited in claim 19, wherein the authentication request is an HDCP authentication request.

21. (Original) Computer program product as recited in claim 19, further comprising:

computer code for retrieving an encrypted authentication key from the non volatile memory corresponding to the authentication request; and

computer code for decrypting the authentication request based upon a corresponding decryption protocol.

22. (Original) Computer program product as recited in claim 21, further comprising:

computer code for responding to the authentication request based on the decrypted authentication request.

New claims

23. (New) A method of using and storing a cryptography key in a display unit, comprising:

retrieving a first encrypted key from a non-volatile memory incorporated in the display unit;

generating a first decrypted key by decrypting the first encrypted key according to a first encryption protocol;

receiving a plurality of pixel data elements encoded in a display signal in an encrypted form that represent an image;

decrypting said encrypted plurality of pixel data elements using the first decrypted key;

generating said plurality of pixel data elements based upon said decrypted plurality of pixel data elements;

displaying said image on a display screen based on said decrypted plurality of pixel data elements;

destroying the first encrypted key;

receiving a second encrypted key from the non-volatile memory that is different from the first encrypted key;

generating a second decrypted key by decrypting the second encrypted key according to a second encryption protocol that is different from the first encryption protocol; and

decrypting said encrypted plurality of pixel data elements using the second decrypted key.

24. (New) A method as recited in claim 23, wherein said display signal is received according to TMDS format.

25. (New) Computer program product executable by a processor for using and storing a cryptography key in a display unit, comprising:

computer code for retrieving a first encrypted key from a non-volatile memory incorporated in the display unit;

computer code for generating a first decrypted key by decrypting the first encrypted key according to a first encryption protocol;

computer code for receiving a plurality of pixel data elements encoded in a display signal in an encrypted form that represent an image;

computer code for decrypting said encrypted plurality of pixel data elements using the first decrypted key;

computer code for generating said plurality of pixel data elements based upon said decrypted plurality of pixel data elements;

computer code for displaying said image on a display screen based on said decrypted plurality of pixel data elements;

computer code for destroying the first encrypted key;

computer code for receiving a second encrypted key from the non-volatile memory that is different from the first encrypted key;

computer code for generating a second decrypted key by decrypting the second encrypted key according to a second encryption protocol that is different from the first encryption protocol;

computer code for decrypting said encrypted plurality of pixel data elements using the second decrypted key; and

computer readable medium for storing the computer code.

26. (New) A method as recited in claim 23, wherein said display signal is received according to TMDS format.